

Yuchen Zhao

Lecturer in Computer Science

Education

- 2013–2017 **Ph.D., Computer Science**, University of St Andrews, St Andrews, UK
- 2011–2013 **M.Sc., Information Security**, Wuhan University, Wuhan, China
- 2007–2011 **B.Eng., Information Security**, Huazhong University of Science and Technology, Wuhan, China

Appointments

- 09/2022– **Lecturer**, Department of Computer Science, University of York, York, UK
- 10/2019– **Research Associate**, Dyson School of Design Engineering, Imperial College London, London, UK
09/2022
- 07/2018– **Research Fellow**, School of Electronics and Computer Science, University of Southampton, Southamp-
10/2019 ton, UK
- 07/2017– **Research Fellow**, Cyber Security Centre, De Montfort University, Leicester, UK
06/2018

Publications

- [1] A. M. Abdelmoniem and Y. Zhao. Knowledge Routing in Decentralized Learning. *IEEE Intelligent Systems*, 40(1):38–44, 2025. <https://doi.org/10.1109/MIS.2024.3505543>.
- [2] Y. Huang, R. Aloufi, X. Cadet, Y. Zhao, P. Barnaghi, and H. Haddadi. Low-Energy On-Device Personalization for MCUs. In *Proceedings of 2024 IEEE/ACM Symposium on Edge Computing*, pages 45–58, Rome, Italy, 2024. <https://doi.org/10.1109/SEC62691.2024.00012>.
- [3] Y. Huang, J. Millar, Y. Long, Y. Zhao, and H. Haddadi. Towards Low-Energy Adaptive Personalization for Resource-Constrained Devices. In *Proceedings of the 4th Workshop on Machine Learning and Systems*, pages 73–80, Athens, Greece, Apr. 2024. <https://doi.org/10.1145/3642970.3655826>.
- [4] Y. Huang, Y. Zhao, A. Capstick, F. Palermo, H. Haddadi, and P. Barnaghi. Analyzing Entropy Features in Time-Series Data for Pattern Recognition in Neurological Conditions. *Artificial Intelligence in Medicine*, page 102821, 2024. <https://doi.org/10.1016/j.artmed.2024.102821>.
- [5] C. Adams, M. Eslamnejad, A. Khadka, A. M'manga, H. Shaw, and Y. Zhao. Auditing AI Systems: A Metadata Approach. In M. Bramer and F. Stahl, editors, *Artificial Intelligence XL, Lecture Notes in Computer Science*, pages 241–246, Cham, 2023. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-47994-6_22.
- [6] M. Niu, Y. Zhao, and H. Haddadi. (Poster) Effective Abnormal Activity Detection on Multivariate Time Series Healthcare Data. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*, Madrid, Spain, Oct. 2023. <https://doi.org/10.1145/3570361.3615741>.
- [7] Y. Huang, Y. Zhao, A. Capstick, F. Palermo, H. Haddadi, and P. Barnaghi. (Preprint) Information Theory Inspired Pattern Analysis for Time-series Data, 2023. Online at <https://arxiv.org/abs/2302.11654>.
- [8] S. Hadjixenophontos, A. M. Mandalari, Y. Zhao, and H. Haddadi. Prism: Privacy preserving healthcare internet of things security management. In *Proceedings of the 2023 IEEE Symposium on Computers and Communications*, pages 919–924, Gammarth, Tunisia, July 2023. <https://doi.org/10.1109/ISCC58397.2023.10218268>.

- [9] Y. Huang, Y. Zhao, H. Haddadi, and P. Barnaghi. Using Entropy Measures for Monitoring the Evolution of Activity Patterns. In *Proceedings of the 2022 IEEE World Forum on Internet of Things*, pages 1–6, Yokohama, Japan, Oct. 2022. <https://doi.org/10.1109/WF-IoT54382.2022.10152050>.
- [10] Y. Zhao, P. Barnaghi, and H. Haddadi. Multimodal Federated Learning on IoT Data. In *Proceedings of the 2022 IEEE/ACM 7th International Conference on Internet-of-Things Design and Implementation*, IoTDI '22, pages 43–54, Milan, Italy, May 2022. <https://doi.org/10.1109/IoTDI54339.2022.00011>.
- [11] Y. Zhao, S. S. Afzal, W. Akbar, O. Rodriguez, F. Mo, D. Boyle, F. Adib, and H. Haddadi. Towards Battery-Free Machine Learning and Inference in Underwater Environments. In *Proceedings of the 23rd Annual International Workshop on Mobile Computing Systems and Applications*, HotMobile '22, page 29–34, Tempe, Arizona, Mar. 2022. <https://doi.org/10.1145/3508396.3512877>.
- [12] Y. Zhao, H. Liu, H. Li, P. Barnaghi, and H. Haddadi. (Preprint) Semi-supervised Federated Learning for Activity Recognition, 2021. arXiv:2011.00851, Online at <https://arxiv.org/abs/2011.00851>.
- [13] F. Palermo, H. Li, A. Capstick, N. Fletcher-Lloyd, Y. Zhao, S. Kouchaki, R. Nilforooshan, D. Sharp, and P. Barnaghi. (Poster) Designing A Clinically Applicable Deep Recurrent Model to Identify Neuropsychiatric Symptoms in People Living with Dementia Using In-Home Monitoring Data. In *NeurIPS '21 Workshop - Bridging the Gap: From Machine Learning Research to Clinical Practice*, 2021. arXiv:2110.09868, Online at <https://arxiv.org/abs/2110.09868>.
- [14] Y. Zhao, H. Haddadi, S. Skillman, S. Enshaeifar, and P. Barnaghi. Privacy-Preserving Activity and Health Monitoring on Databox. In *Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking*, EdgeSys '20, pages 49–54, Heraklion, Greece, Apr. 2020. <https://doi.org/10.1145/3378679.3394529>.
- [15] Y. Zhao and I. Wagner. Using Metrics Suites to Improve the Measurement of Privacy in Graphs. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 19(1):259–274, Jan. 2022. (first published on 13 Mar 2020), <https://doi.org/10.1109/TDSC.2020.2980271>.
- [16] T. Blount, L. Koesten, Y. Zhao, and E. Simperl. Understanding the Use of Narrative Patterns by Novice Data Storytellers. In *Proceedings of the 4th International Conference on Computer-Human Interaction Research and Applications*, pages 128–138, 2020. <https://doi.org/10.5220/0010121601280138>.
- [17] Y. Zhao, T. Blount, L. Koesten, and E. Simperl. Structured and Uncertainty-Aware Data Storytelling. In *CHI '19 Workshop on HCI for Accurate, Impartial and Transparent Journalism: Challenges and Solutions*, Glasgow, UK, May 2019. Online at <https://bit.ly/3bSkuVh>.
- [18] Y. Zhao and I. Wagner. On the Strength of Privacy Metrics for Vehicular Communication. *IEEE Transactions on Mobile Computing (TMC)*, 18(2):390–403, Feb. 2019. (first published on 03 May 2018), <https://doi.org/10.1109/TMC.2018.2830359>.
- [19] Y. Zhao and I. Wagner. Poster: Evaluating Privacy Metrics for Graph Anonymization and De-Anonymization. In *Proceedings of the 2018 Asia Conference on Computer and Communications Security*, ASIACCS '18, pages 817–819, Incheon, Republic of Korea, 2018. <https://doi.org/10.1145/3196494.3201586>.
- [20] Y. Zhao. *Recommending Privacy Preferences in Location-sharing Services*. PhD thesis, University of St Andrews, June 2017.
- [21] Y. Zhao, J. Ye, and T. Henderson. A Robust Reputation-Based Location-Privacy Recommender System Using Opportunistic Networks. In *Proceedings of the 8th EAI International Conference on Mobile Computing, Applications and Services*, MobiCASE'16, pages 62–73, Cambridge, Great Britain, 2016. <https://doi.org/10.4108/eai.30-11-2016.2267031>.
- [22] Y. Zhao, J. Ye, and T. Henderson. The Effect of Privacy Concerns on Privacy Recommenders. In *Proceedings of the 21st International Conference on Intelligent User Interfaces*, IUI '16, pages 218–227, Sonoma, California, USA, Mar. 2016. <https://doi.org/10.1145/2856767.2856771>.
- [23] Y. Zhao. Usable Privacy in Location-Sharing Services. In *Companion Publication of the 21st International Conference on Intelligent User Interfaces*, IUI '16 Companion, pages 110–113, Sonoma, California, USA, Mar. 2016. <https://doi.org/10.1145/2876456.2876458>.

- [24] Y. Zhao, J. Ye, and T. Henderson. Privacy-Aware Location Privacy Preference Recommendations. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, MOBIQUITOUS '14, pages 120–129, London, United Kingdom, Dec. 2014. <https://doi.org/10.4108/icst.mobiquitous.2014.258017>.
- [25] Y. Zhao, J. Ye, and T. Henderson. (Poster) Recommending Location Privacy Preferences in Ubiquitous Computing. In *Proceedings of the 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '14, Oxford, United Kingdom, July 2014. Online at <http://hdl.handle.net/10023/5075>.

Service

Technical programme committees

- 2025 **Program committee, The 5th Workshop on Machine Learning and Systems (EuroMLSys), March, 2024, Rotterdam, Netherlands**
- 2024 **Program committee, The 14th International Conference on the Internet of Things, November, 2024, Oulo, Finland**
Program committee, The 33rd International Conference on Computer Communications and Networks (ICCCN '24), July, 2024, Big Island, Hawaii, USA
- 2023 **Program committee, The 32nd International Conference on Computer Communications and Networks (ICCCN '23), July, 2023, Honolulu, Hawaii, USA**
- 2022 **Program committee, The 2nd IEEE/IFIP International Workshop on Internet of Things Management (Manage-IoT '22, co-located with IEEE/IFIP NOMS '22), April, 2022, Budapest, Hungary**
- 2021 **Program committee, The 1st Workshop on Security and Privacy for Mobile AI (MAISP '21, co-located with ACM MobiSys '21), 24 June, 2021, Online, Worldwide**
- 2020 **Program committee, The 14th ACM Conference on Recommender Systems (RecSys '20), 22-26 September, 2020, Online, Worldwide**
- 2019 **Program committee, Demo & LBR of the 27th ACM Conference on User Modelling, Adaption and Personalization (UMAP '19), 9-12 June, 2019, Larnaca, Cyprus**
Program committee, The 27th ACM Conference on User Modelling, Adaption and Personalization (UMAP '19), 9-12 June, 2019, Larnaca, Cyprus
- 2018 **Poster committee, The 16th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys '18), 10-15 June, 2018, Munich, Germany**

Organising Committee

- 2020 **Local arrangements co-chairs, The 26th Annual International Conference on Mobile Computing and Networks (MobiCom '20), 21-25 September, 2020, London, United Kingdom**

Reviewer

- 2024 **IEEE Transactions on Knowledge and Data Engineering**
Journal of Information Security and Applications
- 2023 **IEEE Internet of Things Journal**
IEEE Transactions on Dependable and Secure Computing
Computer & Security
IEEE Transactions on Big Data
- 2022 **IEEE Transactions on Computers**
Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies
ACM Transactions on Privacy and Security
ACM Transactions on Computing for Healthcare
- 2021 **IEEE Transactions on Information Forensics and Security**
IEEE Transactions on Big Data
- 2020 **IEEE Transactions on Big Data**
Computers & Security
- 2018 **Computer Communications**

Journal of Information Security and Applications

2016 **The 13th International Conference on Wirtschaftsinformatik**, February 12-15, 2017, St. Gallen, Switzerland

Policy & Internet

2015 **The 12th IEEE International Conference on Ubiquitous Intelligence and Computing (UIC '15)**, August 10-14, 2015, Beijing, China

The 7th EAI International Conference on Mobile Computing, Applications and Services (MobiCASE '15), November 12-13, 2015, Berlin, Germany

Student Volunteer

2016 **The 8th EAI International Conference on Mobile Computing, Applications and Services (MobiCASE '16)**, Cambridge, UK

The 21st International Conference on Intelligent User Interface (IUI '16), Sonoma, CA, USA

Talks

2021 **"Federated Learning in the Wild"**, Brave Research Reading Session, Online

"Smart Healthcare using IoT Data and Machine Learning", Sensing and the Internet of Things, Online

"IoT Technology based Solutions to Challenges in Healthcare", ULTRATOOL-IoT Student Project, Online

2020 **"IoT Technology based Solutions to Challenges in Healthcare"**, Sensing and the Internet of Things, Online

"Privacy-preserving Activity and Health Monitoring on Databox", The Third ACM International Workshop on Edge Systems, Analytics and Networking, Online

2018 **"Human Data Interaction"**, WAIS Seminar, Southampton

2017 **"A Robust Reputation-based Location-privacy Recommender System using Opportunistic Networks"**, The Scottish Networking Event (SCONE), Glasgow

2016 **"A Robust Reputation-based Location-privacy Recommender System using Opportunistic Networks"**, The 8th EAI International Conference on Mobile Computing, Applications and Services, Cambridge

"Usable Privacy in Location-Sharing Services", The Student Consortium of the 21st International Conference on Intelligent User Interfaces, Sonoma

"The Effect of Privacy Concerns on Privacy Recommenders", The 21st International Conference on Intelligent User Interfaces, Sonoma

2014 **"Privacy-aware Location-privacy Preference Recommendations"**, The 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, London

"Privacy-aware Location-privacy Preference Recommendations", The Scottish Networking Event (SCONE), Edinburgh

Funding

2023 **Building a Minimal Viable Digital Identity from Digital Footprints (Co-I)**, EPSRC SPRITE+ Sandpit, 4 months, £35.9k

AI Testing Innovation (Expert Panel), Innovate UK Transformative Technologies, 6 months, £49.9k

2013–2017 **600th Anniversary Scholarship (award rate = 7/80)**, University of St Andrews

2016 **IUI 2016 Student Travel Grant**

Student Supervision

21–22 (ICL) **Ph.D (as assistant supervisor)**, Mengjia Niu

21–22 (ICL) **Ph.D (as assistant supervisor)**, Yushan Huang

Teaching

- 24–25 (York) **Lecturer (Module Lead)**, NETS (Network Security)
Lecturer, EHAC (Ethical Hacking)
- 23–24 (York) **Lecturer (Module Lead)**, NETS (Network Security)
- 22–23 (York) **Lecturer (Module Lead)**, NETS (Information & Network Security)/NTAC (Networks & Communications Security: Threats, Attacks & Countermeasures)
Lecturer, CRES (Cyber Security Research Skills)
Mentor, WASP (Wider Aspects of Cyber Security)
- 21–22 (ICL) **Guest lecturer**, Sensing and Internet of Things
- 20–21 (ICL) **Guest lecturer**, Sensing and Internet of Things
Tutor, Design Engineering Futures
- 18–19 (Soton) **Tutor**, COMP6234 (Data Visualisation)
- 16–17 (StA) **Demonstrator**, CS1002 (Object-Oriented Programming)
Demonstrator, CS2001 (Foundations of Computation)
Demonstrator, CS2003 (The Internet and the Web: Concepts and Programming)
- 15–16 (StA) **Tutor**, CS1002 (Object-Oriented Programming)
Tutor, CS1006 (Programming Projects)
Demonstrator, CS1002 (Object-Oriented Programming)
Demonstrator, CS2001 (Foundations of Computation)
Demonstrator, CS2003 (The Internet and the Web: Concepts and Programming)
- 14–15 (StA) **Tutor**, CS1006 (Programming Projects)
Demonstrator, CS1002 (Object-Oriented Programming)
Demonstrator, CS1003 (Programming with Data)
Demonstrator, CS1006 (Programming Projects)
Demonstrator, CS2003 (The Internet and the Web: Concepts and Programming)